UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

United States of America,

Plaintiff,

v. Case No. 1:15cr109

Richard Stamper, Judge Michael R. Barrett

Defendant.

OPINION & ORDER

This matter is before the Court upon Defendant's Motion to Dismiss or Alternatively Suppress Evidence. (Doc. 33, SEALED). The Government filed a Response. (Doc. 34, SEALED). This Court held a hearing on the Motion on January 28, 2016. (Doc. 38). Defendant filed a Supplemental Post-Hearing Memorandum. (Doc. 39). The Government filed a Supplemental Memorandum (Doc. 40), to which Defendant filed a Response (Doc. 41, SEALED).

I. BACKGROUND

Defendant Richard Stamper has been charged with receipt and possession of child pornography in violation of 18 U.S.C. § 2252(a)(2), (a)(4), (b)(1) and (b)(2). These charges stem from an investigation conducted by Special Agents with the Federal Bureau of Investigation ("FBI") which led to the discovery of a website known as "Playpen." The Government alleges that the website, also referred to as "Website A" or "Target Website," contains child pornography. Website A was operating on an internet network known as

the Tor, or "the Onion Router." The Tor network allows users to hide identifying information such as Internet Protocol addresses ("IP addresses"). One court has described how the Tor functions:

> Tor directs internet traffic through a free, worldwide network of relays to conceal a user's location or usage from anyone attempting network surveillance or traffic analysis. Tor involves the application of layers of encryption (nested like layers of an onion) to anonymize communication by sending the original data to its destination without revealing the source IP address making it impossible to trace the communications back through the network to the actual user who sent the communication.

United States v. Pierce, No. 8:13CR106, 2014 WL 5173035, at *3 (D. Neb. Oct. 14, 2014). Because Website A was operating on the Tor, as opposed to the "open" internet, the website could only be accessed if the user knew the web address of the website. (See Doc. 33-1, NIT Search Warrant Aff. ¶10).

Based on information from foreign law enforcement, the FBI determined that the computer server which hosted Website A was located at a web-hosting facility in North Carolina. (Doc. 33-1, NIT Search Warrant Aff. ¶ 28). The FBI obtained a Title III warrant to seize the server containing Website A. (Id.) The FBI allowed Website A to continue to operate, but assumed administrative control of the website from a government-controlled server located in Newington, Virginia. (See Doc. 33-1, NIT Search Warrant Aff. ¶ 30).[1]

FBI agents also obtained a search warrant from a magistrate judge in the Eastern District of Virginia authorizing the use of a "network investigative technique" ("NIT") to be

[1]The NIT warrant itself stated that upon seizure of the server, the server operating Website A "will be located at a government facility in the Eastern District of Virginia." (See Doc. 33-1, Attachment A).

deployed on the computer server. (Doc. 33-1, Attachment A) ("the NIT warrant"). The NIT warrant provided that once the NIT was deployed on the computer server, it would obtain information from the activating computers. (Id., Attachment A). Activating computers are the computers of users or administrators who log in with a user name and password to Website A. (Id.) Each time a user or administrator logged in to Website A, the NIT attempted to cause the activating computer to send specific information to a government-controlled computer located in the Eastern District of Virginia. (Doc. 33-1, NIT Search Warrant Aff. ¶ 36).

The NIT warrant limited the information to be seized by the NIT from the activating computers to information listed in Attachment B to the warrant: 1) the activating computer's "actual IP address and the date and time that the NIT determines what the IP address is;" 2) "a unique identifier generated by the NIT…to distinguish data from that of other 'activating' computers;" 3) the type, version and architecture of the operating system running on the computer; 4) "information about whether the NIT has already been delivered to the 'activating' computer;" 5) "the 'activating' computer's Host Name;" 6) "the 'activating' computer's active operating system username;" and, 7) "the 'activating' computer's media access control ('MAC') address." (Doc. 33-1, Attachment B).

As a result of the NIT warrant, the FBI discovered that on February 3, 2015, a user registered for an account on Website A using the username "billnyepedoguy." (Doc. 32-1, Residential Search Warrant Affidavit, ¶ 27). The Government explains that according to the statistics section of this user's profile, the user "billnyepedoguy" had been actively logged into the website for a total of four hours, one minute and 57 seconds,

between February 3, 2015 and March 4, 2015. (Id.) The FBI also identified the IP address and MAC Address used by "billnyepedoguy" to log into Website A; and determined "billneypedoguy" used the host name of "badass" and log-on ID of "richard." (Id., ¶ 28).

Using publicly available websites, the FBI was able to determine that the IP address associated with the user "billnyepedoguy" was operated by the internet service provider Time Warner Cable. (Doc. 32-1, Residential Search Warrant Affidavit, ¶ 34). An administrative subpoena was served on Time Warner Cable requesting information related to the user who was assigned to the IP address during the dates and times the user "billnyepedoguy" was accessing Website A. (Id.) The results of the subpoena showed that Defendant was the subscriber of the IP address. (Id., ¶ 35). In September of 2015, law enforcement agents obtained a search warrant from a magistrate judge in this district for Defendant's home. Defendant has challenged this residential search warrant in a separate motion. (See Doc. 32, Motion to Suppress Evidence Seized Pursuant to SD Ohio Search Warrant).

Defendant moves to dismiss the indictment in this matter, or alternatively to suppress the evidence seized pursuant to the NIT warrant issued in the Eastern District of Virginia. Defendant argues that the magistrate judge in the Eastern District of Virginia did not have jurisdiction to issue a warrant allowing a NIT search of a computer in the Southern District of Ohio, or in any jurisdiction outside of the Eastern District of Virginia. Defendant explains that as a result, this Court must dismiss the indictment in this case. In the alternative, Defendant requests that the Court suppress the evidence seized as a

result of the NIT warrant and the fruits of that search based on violations of the Fourth Amendment.

II. ANALYSIS

A. Fourth Amendment

The Fourth Amendment prohibits "unreasonable searches and seizures" and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend IV. "As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is reasonableness." *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995) (internal quotation marks omitted).

The Sixth Circuit has recognized the difficulty in applying the Fourth Amendment's particularity requirement in the context of a search of a computer: "[t]he problem with applying this [requirement] to computer searches lies in the fact that [ ] images could be nearly anywhere on the computers. Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents." *United States v. Evers*, 669 F.3d 645, 653 (6th Cir. 2012) (quoting *United States v. Richards,* 659 F.3d 527, 538, n.8 (6th Cir. 2011)). As a consequence:

> given the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis: "While officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant, ... a computer search may be as

> extensive as reasonably required to locate the items described in the warrant based on probable cause." *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir.), *cert. denied*, 558 U.S. 1097, 130 S.Ct. 1028, 175 L.Ed.2d 629 (2009) (citations and internal quotation marks omitted).

Id. (quoting *Richards*, 659 F.3d at 538 (footnotes omitted)); *see also United States v. Ganias*, 755 F.3d 125, 134 (2d Cir. 2014) ("Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools."); *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006) ("The fact of an increasingly technological world is not lost upon us as we consider the proper balance to strike between protecting an individual's right to privacy and ensuring that the government is able to prosecute suspected criminals effectively.").

Defendant's Motion centers on Federal Rule of Criminal Procedure 41(b). Defendant argues that under Rule 41(b), a magistrate judge's authority to issue a search warrant is limited to their own judicial district except under certain narrow circumstances.[2]

---

[2]Federal Rule of Criminal Procedure 41(b) provides in relevant part:

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> (3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism

Defendant explains that none of those circumstances exist in this case.

The Sixth Circuit has explained "[a]lthough the purpose of Rule 41 is the implementation of the fourth amendment, the particular procedures it mandates are not necessarily part of the fourth amendment." *United States v. Searp*, 586 F.2d 1117, 1121 (6th Cir. 1978), *cert. denied* 440 U.S. 921 (1979). Even where there is a failure to comply with Rule 41, a search may nevertheless be "reasonable" in the constitutional sense and meet the requirements of the Fourth Amendment. *Id*. at 1122. For this reason, the Sixth Circuit has instructed that "'[v]iolations of Rule 41 alone should not lead to exclusion unless (1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.'" *Id.* at 1125 (quoting

---

> may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
>
> (A) a United States territory, possession, or commonwealth;
>
> (B) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

United States v. Burke, 517 F.2d 377, 386-87 (2d Cir.1975)).

The handful of federal courts which have addressed the issue agree with Defendant and have found that a search warrant authorizing the use of a NIT does not comply with Rule 41.[3] However, these courts, with one exception, have found that the search is nevertheless "reasonable" and does not violate the Fourth Amendment.

B. Judicial precedent and NIT search warrants

1. *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013).

In *In re Warrant to Search a Target Computer at Premises Unknown*, an unknown person accessed a personal email account and used that email address to access the bank account of a man residing within the jurisdiction of the federal district court for the Southern District of Texas. 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013). The IP address of the computer which accessed these accounts came from a foreign country, but the location of the suspects and their computer was unknown. *Id*. The government requested a warrant authorizing: (1) a search for the target computer itself, and (2) a search for digital information stored on (or generated by) that computer. *Id*. at 757. The government sought to install data extracting software that had "the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to the FBI." *Id*. at 755.

[3]The absence of a provision permitting these types of searches has prompted calls for revisions to be made to Rule 41. *See* Brian L. Owsley, Beware of Government Agents Bearing Trojan Horses, 48 Akron L. Rev. 315, 344 (2015) (explaining that the Department of Justice has proposed a change to Rule 41 to authorize search warrants using NITs).

The magistrate judge denied the application for the search warrant on three different grounds. First, the magistrate judge concluded that the warrant application did not satisfy any of the territorial limits found in Federal Rule of Criminal Procedure 41(b). The magistrate judge rejected the government's argument that the search warrant satisfied Rule 41(b)(1)—which authorizes a magistrate judge to issue a warrant to search property located within the district—because the information obtained from the target computer would be examined by the government within the magistrate judge's judicial district. *Id*. at 756. The magistrate judge explained:

> The "search" for which the Government seeks authorization is actually two-fold: (1) a search for the Target Computer itself, and (2) a search for digital information stored on (or generated by) that computer. Neither search will take place within this district, so far as the Government's application shows. Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location. Before that digital information can be accessed by the Government's computers in this district, a search of the Target Computer must be made. That search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name. Since the current location of the Target Computer is unknown, it necessarily follows that the current location of the information on the Target Computer is also unknown. This means that the Government's application cannot satisfy the territorial limits of Rule 41(b)(1).

Id. at 757 (footnote omitted).

Next, the magistrate judge found that the warrant application did not satisfy the particularity requirement of the Fourth Amendment because the government failed to give any explanation of how the target computer would be found, or how the government's search technique would avoid infecting innocent computers and devices. *Id*. at 758-59.

Finally, the magistrate judge noted that the software described in the warrant

application would be able to access the computer's build-in camera to engage in "photo monitoring." *Id*. at 769. The magistrate judge explained that this type of access amounts to video surveillance, and would need to satisfy the Fourth Amendment warrant standards for video surveillance. *Id*. at 759-760. The magistrate judge concluded that the government had not met these standards. *Id*. at 760. Specifically, the government had not shown that other alternative investigative techniques were inadequate or that steps would be taken to minimize over-collection of data. *Id*.[4]

The magistrate judge noted that "there may well be a good reason to update the territorial limits of [Rule 41(b)] in light of advancing computer search technology." *Id*. at 761. However, the magistrate judge explained that "the extremely intrusive nature of such a search requires careful adherence to the strictures of Rule 41 as currently written, not to mention the binding Fourth Amendment precedent for video surveillance." *Id*. at 761.

2. *United States v. Pierce*, 2014 WL 5173035 (D. Neb. Oct. 14, 2014).

A year later, in *United States v. Pierce*, the federal district court for Nebraska denied a motion to suppress evidence derived from a NIT search warrant. Nos. 8:13CR106, 8:13CR107, 8:13CR108, 2014 WL 5173035, at *3 (D. Neb. Oct. 14, 2014). The warrant authorized the FBI to deploy a NIT on a child pornography website operating from computers in Nebraska that used the Tor network for anonymity. *Id*. Once the NIT was installed on the website and the user accessed the website, the NIT sent out one or

[4]With regards to alternatives, the magistrate judge noted that "contemporaneous with this warrant application, the Government also sought and obtained an order under 18 U.S.C. § 2703 directing the Internet service provider to turn over all records related to the counterfeit email account, including the contents of stored communications." 958 F. Supp. 2d at 760.

more communications to the user's computer. *Id*. The user's computer then delivered information, such as the IP address, to a computer controlled by the FBI. *Id*. Administrative subpoenas were issued to the internet service providers to identify the owners of the IP addresses, which led to individual search warrants and charges against the defendants. *Id*.

The defendants did not challenge the probable cause for the issuance of the NIT warrant. *Id*. Instead, the defendants argued that the language in the warrant providing for notice to be delayed for thirty days violated Federal Rule of Criminal Procedure 41. *Id*. The court rejected this argument because the warrant clearly contemplated a period of thirty days after the discovery of an IP address to determine ownership of the computer connected to that address. *Id*. at *4. In the alternative, the court concluded that the defendants failed to demonstrate prejudice or reckless disregard of proper procedure.[5]

3. *United States v. Reibert*, 2015 WL 366716 (D. Neb. Jan. 27, 2015).

A few months later, in *United States v. Reibert*, the federal district court for the District of Nebraska again denied a motion to suppress evidence derived from a NIT search warrant. No. 8:13CR107, 2015 WL 366716, at *2 (D. Neb. Jan. 27, 2015). The NIT search warrant authorized the government to deploy the NIT on a website which was dedicated to advertising and distributing child pornography. *Id*. at *4. The website operated on the Tor network in order to mask the users' actual IP addresses. *Id*. Once the NIT was deployed, each time a user accessed the website, the NIT sent one or more

[5]The court explained that under Eighth Circuit law: "when the government does not comply with the requirements of Rule 41, exclusion is warranted only if: (1) the defendant can demonstrate that he was prejudiced, or (2) 'reckless disregard of proper procedures is evident.'" 2014 WL 5173025, at *5 (quoting *United States v. Spencer*, 439 F.3d 905, 913 (8th Cir. 2006)).

communications to the user's computer which would then cause the computer to send information, such as its IP address, to a government-controlled computer. *Id*. at *5. Based on this information, the FBI obtained a residential search warrant for the defendant's home in Ohio. *Id*.

The defendant argued that the government conducted a warrantless search by employing a NIT. *Id*. at *1. The defendant also argued that the NIT search warrant lacked probable cause. *Id*. The court rejected these arguments and cited Eighth Circuit caselaw which found probable cause existed where child pornography is traced to the defendant using an IP address. *Id*. at *3. In the alternative, the court concluded that even if the NIT search warrant was not supported by probable cause, the good faith exception to the exclusionary rule identified in *United States v. Leon*, 468 U.S. 897, 922 (1984), would apply. *Id*. at *3.

4. *United States v. Welch*, 2016 WL 240775 (8th Cir. Jan. 21, 2016).

Just a few weeks ago, the Eighth Circuit affirmed the district court's denial of the motion to suppress in *United States v. Pierce*, 2014 WL 5173035 (D. Neb. Oct. 14, 2014). On appeal, one of the co-defendants argued that the district court erred in admitting evidence obtained as a result of the NIT search warrant because he was provided notice beyond thirty days in violation of Federal Rule of Criminal Procedure 41. *United States v. Welch*, 2016 WL 240775, at *2 (8th Cir. Jan. 21, 2016).

The Eighth Circuit began its analysis by noting: "Importantly, a Rule 41 violation amounts to a violation of the Fourth Amendment warranting exclusion 'only if a defendant is prejudiced or if reckless disregard of proper procedure is evident.'" *Id*. (quoting *United*

States v. Spencer, 439 F.3d 905, 913 (8th Cir. 2006)). The Eighth Circuit assumed, without deciding, that Rule 41 applied to the NIT search warrant. *Id*. at *3. The court explained that it was still an open question as to whether the defendant's IP address—which is generated by a third party and assigned by the internet service provider—is the kind of "information" considered to be property under Rule 41. *Id*. at n.4. The court concluded that the notice given to the defendant did not comport with Rule 41. *Id*. However, the court concluded that the delay in notice appeared to be an error made in good faith and not a deliberate procedural violation. *Id*. The court also concluded that there was no evidence of prejudice: "Nothing in the record indicates that had the officers followed Rule 41 they would not have been able to search Welch's residence and obtain the evidence they did. The nature of the investigation indicates they could have easily obtained extensions had they sought them." *Id*. at *4. Therefore, the court concluded that the delayed notice to the defendant of the NIT warrant did not violate the Fourth Amendment. *Id*.

5. *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

More recently, on January 28, 2016, the federal district court for the Western District of Washington denied a motion to suppress evidence based on the same NIT search warrant which is being challenged in this case. *United States v. Michaud*, No. 3:15CR5351, 2016 WL 337263, *3 (W.D. Wash. Jan. 28, 2016).

The defendant in *Michaud* raised two Fourth Amendment arguments: whether deploying the NIT from the Eastern District of Virginia, to the defendant's computer, located outside that district, exceeded the scope of the NIT warrant's authorization; and

whether the NIT warrant lacks particularity and amounts to a general warrant. *Id*. at *3. The defendant also argued that the NIT warrant violated Federal Rule of Criminal Procedure 41(b).

As to the first argument, regarding the scope of the NIT warrant, the court explained: "Whether a search or seizure exceeds the scope of a warrant is an issue that is determined 'through an objective assessment of the circumstances surrounding the issuance of the warrant, the contents of the search warrant, and the circumstances of the search.'" *Id*. at *3 (quoting *U.S. v. Hurd*, 499 F.3d 963, 966 (9th Cir. 2007)). The court explained that "while the NIT Warrant cover sheet does explicitly reference the Eastern District of Virginia, that reference should be viewed within context." *Id*. at *4.[6] The court explained that in the blank space on the warrant where the magistrate judge is to "give its location," the blank has been filled in with "See Attachment A." *Id*. The court explained further that:

> Attachment A, subtitled "Place to be Searched," authorizes deployment of the NIT to "all activating computers," defined as "those of any user or administrator who logs into [Website A] by entering a username and password." *Id*. Attachment A refers to the Eastern District of Virginia as the location of the government-controlled computer server from which the NIT is deployed. *Id*. A reasonable reading of the NIT Warrant's scope gave the FBI authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto

---

[6]The cover sheet for the warrant stated:

> An application by a federal law enforcement officer...requests the search of the following person of property located in the Eastern District of Virginia (*identify the person or describe the property to be searched and give its location*):
>
> See Attachment A

Id. at *4.

> Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia.

Id. The court explained that the warrant application reinforces this objectively reasonable interpretation because when detailing how the NIT works, the warrant application explains that the NIT "may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government [in the Eastern District of Virginia], *network level messages containing information that may assist in identifying the computer, its location*, and other information[.]" *Id*. (emphasis added).

As to the second argument, that the NIT warrant lacks particularity and amounts to a general warrant, the court explained that whether a warrant lacks specificity depends on two factors: particularity and breadth. *Id*. (citing *United States v. SDI Future Health, Inc*., 568 F.3d 684, 702 (9th Cir. 2009)). The court concluded that the NIT warrant was not lacking in particularity and did not exceed the breadth—or scope—of the probable cause on which it was based. *Id*. at *5. The court also concluded that even if the NIT Warrant was unconstitutional because it is a general warrant, suppression may not be required under *United States v. Leon*, 468 U.S. 897 (1984) because the officers were acting in good faith when executing the warrant. *Id*.

As to the final argument, that the NIT warrant violates Rule 41(b), the court found that the NIT technically violated the letter, but not the spirit of the rule. *Id*. The court explained: "The rule does not directly address the kind of situation that the NIT Warrant was authorized to investigate, namely, where criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI in a known location." *Id*. at *6.

The court explained that because there was a technical violation of the Rule, and not a violation of a constitutional magnitude: "courts may suppress where a defendant suffers prejudice, 'in the sense that the search would not have occurred...if the rule had been followed,' or where law enforcement intentionally and deliberately disregarded the rule." *Id*. (quoting *United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005)). The court clarified that "prejudice" meant considering "whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means." *Id*. (citing *United States v. Vasser*, 648 F.2d 507, 511 (9th Cir. 1980)).

The court found that the defendant did not suffer prejudice:

> Mr. Michaud has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Although the IP addresses of users utilizing the Tor network may not be known to websites, like Website A, using the Tor network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific physical location. Even though difficult for the Government to secure that information tying the IP address to Mr. Michaud, the IP address was public information, like an unlisted telephone number, and eventually could have been discovered.

Id. at *7. The court also found that the FBI did not act intentionally and with deliberate disregard of Rule 41(b). *Id*. Therefore, the court found that even if the NIT warrant was invalid, the FBI executed the warrant in good faith under *United States v. Leon*, 468 U.S. 897 (1984). *Id*. Accordingly, the court denied the defendant's motions to suppress. *Id*. at *8.

C. The NIT search warrant in this case

Defendant argues that *Michaud* is distinguishable because the district court in that case is applying Ninth Circuit caselaw. Defendant argues that even under the Ninth Circuit's analysis, suppression of evidence is warranted because Defendant suffered prejudice and law enforcement deliberately disregarded Rule 41(b). Finally, Defendant argues that the good faith exception does not save the warrant because the warrant was facially insufficient and it is clear from the facts that the agents knew the limits of the territorial jurisdiction of the court and ignored them when they obtained and executed the warrant.

1. Scope of the NIT Search Warrant

There is little to distinguish the facts of this case from *Michaud*. The Court also notes that there is little difference between the Ninth Circuit and the Sixth Circuit with regards to the applicable caselaw. Finally, the Court finds that the legal conclusions reached by the court in *Michaud* are in line with the courts which have addressed similar NIT search warrants. The Court finds *Michaud* persuasive.

The Court agrees that "a reasonable reading of the NIT Warrant's scope gave the FBI authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia." *Michaud*, 2016 WL 337263, *4. The Sixth Circuit has explained that "when examining the legitimacy of search warrants, we are to follow a commonsensical and practical approach, as opposed to an overly technical review." *United States v. Bennett*,

170 F.3d 632, 639 (6th Cir. 1999) (citing *United States v. Ventresca*, 380 U.S. 102, 108, 85 S.Ct. 741, 746, 13 L.Ed.2d 684 (1965)). When the Government sought the NIT warrant, Website A was being operated from a government-controlled computer in the Eastern District of Virginia. While the NIT did send information to the activating computers, this only occurred after a user logged into the website. Any information sent by the activating computer was sent back to the Eastern District of Virginia. The information sent by the activating computer was limited and specified in the NIT warrant. This process was described in great detail in the NIT Search Warrant Affidavit:

> In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant, the TARGET WEBSITE, which will be located in Newington, Virginia, in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from the TARGET WEBSITE, located in the Eastern District of Virginia, the instructions, which comprise the NIT, are designed to cause the user's "activating" computer to transmit certain information to a computer controlled by or known to the government. That information is described with particularity on the warrant (in Attachment B of this affidavit), and the warrant authorizes obtaining no other information.

(Doc. 33-1, Search Warrant Aff. ¶ 33). Defendant has not argued that the search conducted by the FBI agents went beyond the scope of what was described in the warrant.[7]

Moreover, the Court finds that the NIT Warrant was reasonable in the scope of the information searched. For this reason, this case is distinguishable from *In re Warrant to*

[7]Therefore, it is unnecessary for the Court to analyze whether the NIT Warrant amounted to a "general warrant." *See United States v. Garcia*, 496 F.3d 495, 507 (6th Cir. 2007) ("The test for determining if the officers engaged in an impermissible general search is whether their search unreasonably exceeded the scope of the warrant.") (citing *Brindley v. Best*, 192 F.3d 525, 531 (6th Cir. 1999)).

Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013), where the issuance of the warrant was denied. In that case, the government sought to install data extracting software that had "the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to the FBI." *Id*. at 755. Here, the search was much less invasive. The information seized by the NIT from the activating computer did not include any information stored on the activating computer or even the location of the computer. The information seized did include the IP address, which did not identify the user of Website A until the FBI agents found the name of the internet service provider and then requested the name of the subscriber through an administrative subpoena. It was not until FBI agents secured a residential search warrant from a magistrate judge in this district that the agents were able to search the content of Defendant's computer. Therefore, the Court concludes that the NIT Warrant was not unconstitutional in its scope and there is no basis to dismiss the indictment in this case, or suppress the evidence seized as a result of the NIT warrant.

2. <u>Good faith</u>

However, even if the Court were to find that the NIT Search Warrant was unconstitutional because the use of the NIT allowed the FBI to extend its search to computers located outside of the Eastern District of Virginia, the Court finds that suppression is not required. The *Leon* good-faith exception, "which allows admission of evidence 'seized in reasonable, good-faith reliance on a search warrant that is

subsequently held to be defective,'" applies in this case. *See United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). Only in exceptional circumstances is the good faith exception inappropriate: (1) if the issuing magistrate was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) if the issuing magistrate failed to act in a neutral and detached fashion and merely served as a rubber stamp for the police; (3) if the affidavit was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable, or where the warrant application was supported by nothing more than a bare bones affidavit; and (4) if the warrant was facially deficient in that it failed to particularize the place to be searched or the things to be seized. *Id*. at 914-15, 923.

Defendant argues that reliance on the warrant was not objectively reasonable because the warrant was facially deficient. Defendant argues that the NIT Warrant failed to particularize the place to be searched or the things to be seized because the FBI agents knew the limits of the territorial jurisdiction of the court and ignored them when they obtained and executed the warrant. Defendant relies on *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013) to support his argument.

In *Glover*, the court found a wiretap warrant facially invalid because it authorized the placement of a listening device, or electronic "bug" on the target vehicle while it was outside the court's jurisdiction. *Id*. at 515. While it may be tempting to analogize the "bug" to the NIT in this case, under that analogy, the NIT was "attached" to activating computers when the user logged into Website A, which was being operated from the

Eastern District of Virginia. It would be as if the users travelled to the Eastern District of Virginia, picked up the bug while they were there, and then carried it back home with them. The Court is not persuaded that the court's conclusion in *Glover* is applicable here. Therefore, the Court finds that even if the NIT Warrant is unconstitutional, the *Leon* good-faith exception allows the admission of the evidence seized as the result of the NIT.

3. Rule 41(b)

Finally, the Court finds that the NIT Warrant technically violates Rule 41(b). *Accord Michaud*, 2016 WL 337263, at *6. However, exclusion is not necessary because there has not been a showing of prejudice or an intentional and deliberate disregard of the Rule. *See United States v. Searp*, 586 F.2d at 1121.

Defendant maintains that he has established prejudice based on two statements in the NIT Search Warrant Affidavit:

> Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and failed or reasonably appear to be unlikely to succeed if they are tried. (Doc. 33-1, Search Warrant Aff. ¶ 31).
>
> The government further submits that, to the extent that the use of the NIT can be characterized as a seizure of an electronic communication or electronic information under 18 U.S.C. § 3103a(b)(2), such a seizure is reasonably necessary, because without this seizure, there would be no other way, to my knowledge, to view the information and to use it to further the investigation. (Doc. 33-1, Search Warrant Aff. ¶ 41).

Defendant argues that based on these statements, the search of his computer would not have occurred if Rule 41(b) had been followed. The Court disagrees. The information

seized by the NIT did not lead to Defendant directly. Instead, the FBI Agents only learned Defendant's IP Address as a result of the NIT Warrant. Defendant did not suffer prejudice by having this information revealed. This Court agrees with the court in *Michaud* on this point:

> Mr. Michaud has no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, Mr. Michaud's assigned IP address, which ultimately led to Mr. Michaud's geographic location. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Although the IP addresses of users utilizing the Tor network may not be known to websites, like Website A, using the Tor network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a specific physical location. Even though difficult for the Government to secure that information tying the IP address to Mr. Michaud, the IP address was public information, like an unlisted telephone number, and eventually could have been discovered.

Michaud, 2016 WL 337263, at *7; *see also Smith v. Maryland*, 442 U.S. 735, 743-44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) ("[The Supreme] Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010) ("Federal courts have uniformly held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.") (internal quotation marks and citations omitted).

Next, the Court finds that there is no evidence of intentional and deliberate disregard of Rule 41(b). The government specifically requested a search warrant authorizing that "the NIT may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government, network level messages

containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer, as described above and in Attachment B." (Doc. 33-1, NIT Search Warrant Affidavit ¶ 46) (emphasis added).

Therefore, even though the NIT Warrant technically violates Rule 41(b), exclusion is not necessary.

III. CONCLUSION

Based on the foregoing, Defendant's Motion to Dismiss or Alternatively Suppress Evidence (Doc. 33, SEALED) is **DENIED**.

IT IS SO ORDERED.

/s/ Michael R. Barrett
Michael R. Barrett, Judge
United States District Court